Defense Information Systems Agency

A Combat Support Agency

Computing Services Technical Architecture

Ms. Ethel Stewart
Technical Director
Computing Services
April 2009

DISA
A Combat Support Agency

Agenda

- **Technology Alignment with Business Strategies**
- **Defense Computing Enterprise Center (DECC) Branding**
- **Enterprise Segment Architecture**
- **Innovative Strategic Approaches**

DISA

A Combat Support Agency

Alignment with Business Strategies

- **Business drivers**
  - **DISA strategic plan**
  - **Cost effective solutions**
  - **Unity of efforts**
- **Technology fusion**
  - **Reduced platforms**
  - **Corporate utility**
  - **Seamless integrated infrastructure**
  - **NetCentric reportability**
  - **Standard Enterprise Architecture**

DISA
A Combat Support Agency

DECC Branding

- **Secure, scalable, computing and storage environments operated inside the DoD network**
  - **Highest level of network defense (DECCs are at the core)**
  - **Computer Network Defense compliant with Information Assurance (IA) policy (e.g. DoD Instruction 8500, Federal Information Security Management Act)**
- **High performance, high availability networks**
  - **Fully redundant and actively monitored networks**
  - **Directly connected to GIG optical backbone**
  - **Unlimited DISN IP backbone connectivity**
- **Full support for NetOps essential tasks (important enabler of NetCentric operations)**
  - **Computer Network Defense**
  - **GIG Enterprise Management**
  - **GIG Content Management**

DISA
A Combat Support Agency

Segment Architecture

- An agile design approach to support business need during continuous change
  - Avoids obsolete architectural design
  - Design architecture in time of need
  - The enterprise architecture on demand
  - Elaborates the target architecture master plan
- Enables incremental and continuous enterprise architecture efforts based on business needs
  - Value delivered to the right people, in the right area, at the right time
- Segment Architecture
  - Core Architectural Foundation
  - Information Assurance Architec
  - Management Architecture
  - Out-of-Band Network
  - Enterprise Systems Manageme
  - Enterprise Back-up Network

DISA
A Combat Support Agency

Standard Core Foundation

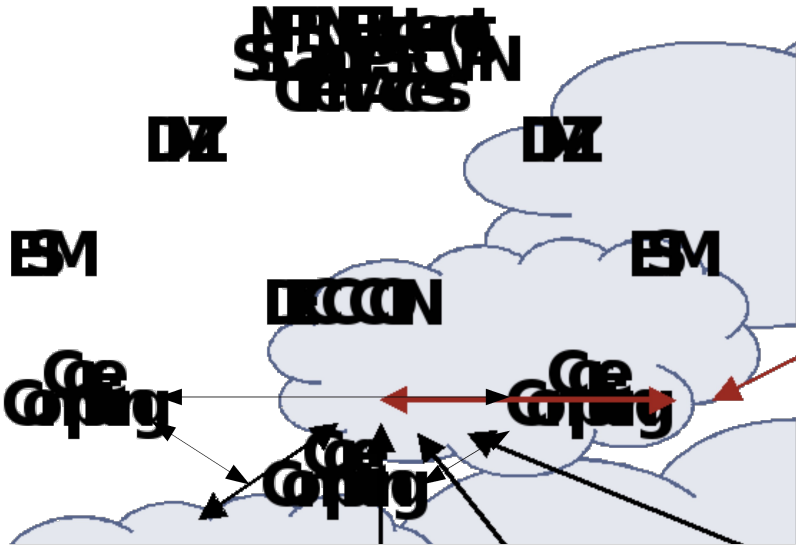
- **Increases efficiencies through established standards**
  - **Standard hardware platforms**
  - **Standard software products**
    - **Monitoring and performance metrics**
    - **Standard Web software**
    - **Standard application software**
    - **Standard database software**
    - **Standard security software**
  - **Standards socialized with Office of the Secretary of Defense**
  - **Virtualization**
    - **Server, network, and storage**
    - **Drives up server utilization, lowers hardware costs**
    - **Cost efficiencies on power, heat, space, full time equivalent**

Seamless Integration for Customers

DISA
A Combat Support Agency

Information Assurance Architecture

- All DECC traffic flows through Demilitarized Zone (DMZ) sites
  - Value added by limiting the access points to our network through one of the DMZs
  - Managed Command and Control
- Example features and benefits
  - Centralized security for DECCs
  - Global-load balancing
  - Application level proxies
  - Secure Sockets Layer (SSL) gateways
  - Transport encryption between all core computing facilities



DISA
A Combat Support Agency

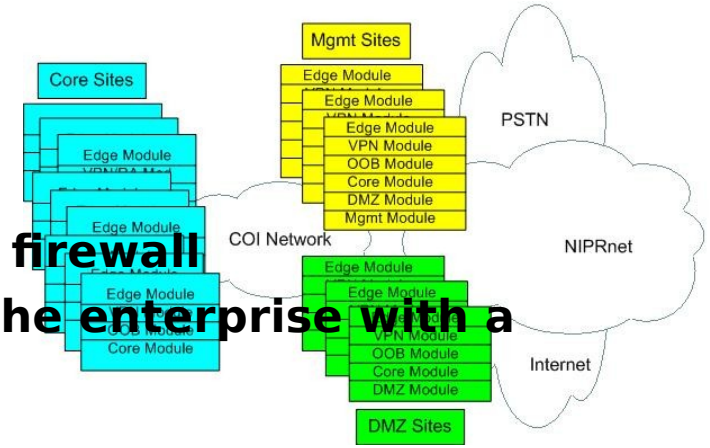
Management Architecture

- One Consolidated Communications Center
  - Virtually distributed, geographically diverse at 4 physical locations
  - Network (enclave and DMZ) operations 24 x 7
- Out-of-Band (OOB) management network
  - Separates system control and monitoring data from production data
- Enterprise Systems Management (ESM)
  - Fault, Configuration, Accounting, and Performance Management
- Identifies and enforces security standards
  - Real Secure, Host Based Security Systems, Policy Enforcement Points, and SCVI-SCRI
- Virtual machine management
  - VMware Virtual Center
- Service Desk
  - Customer aligned
  - Functionally aligned

Out-of-Band (OOB) Network

A Combat Support Agency

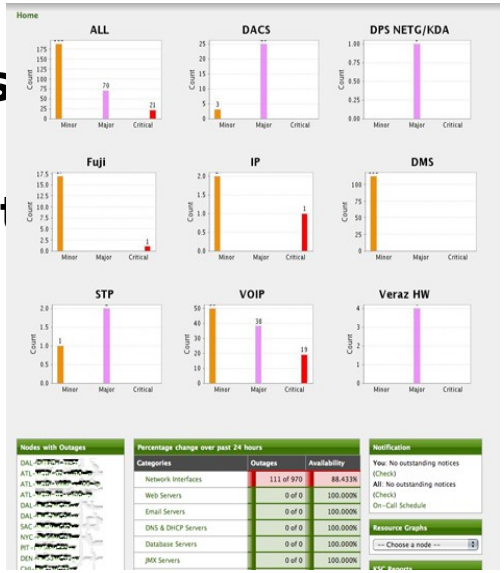
- Created with Virtual Private Network (VPN) connections
  - Site-to-site from all sites to ESM sites
    - Provides path for production hosts to send/receive ESM traffic
  - SSL/Internet Protocol Security (IPSEC) client mode VPNs, SA to host
    - Authorized users utilize Web SSL or IPSEC VPN client apps to connect to the OOB
    - Admission criteria requires a valid CAC and a radius user name/password
    - For non-trusted networks, split tunnel is disabled
- IA architecture and OOB
  - Flows through DMZs
  - All access points via SSL VPN client
  - Provides high availability access
  - Adds an additional security layer via a firewall
  - The ability to manage devices across the enterprise with a single login



DISA
A Combat Support Agency

Enterprise Systems Management (ESM)

- ESM suite of tools to manage the needs of our computing environments
- Data collectors provide an overall view of the health and status of IT resources
  - Networks, systems, applications and databases
- Effective management of HW and SW
  - Inventory scanning, reporting, SW development and deployment
- Centralization improves the ratio of systems analysts to servers
  - Monitoring and management of global IT asset
  - Reduces cost, saves on licensing costs
  - Emphasizes integration of multiple diverse systems into a standard infrastructure
  - Facilitates changes and eases burden of troubleshooting efforts



DISA
A Combat Support Agency

Enterprise Back-up Network (EBN)

- EBN is a separate network designed to isolate back-up activity and traffic (OOB, Production)
- Cost effective solution
  - Gigabit Ethernet
  - Veritas based with centralized master/media servers
  - Gigabit NIC cards switches versus fibre channel

- Digital Linear Tape (DLT)/Super DLT media transitioning to Linear Tape Open-3 media-based tape libraries
- Host traffic restricted to master/media servers
  - No host to host communications
- The OOB network is used to manage backups remotely

DISA
A Combat Support Agency

Innovative Strategic Approaches

- Capacity Services
  - Computing Platforms and Operating Systems
  - Storage
- Rapid Access Computing Environment (RACE)
  - 24 hour online provisioning
  - Path to Production
- IaaS (Infrastructure-as-a-Service)
  - DoD DMZ
  - DISA Extended Edge Presence
  - GIG Content Delivery Service
- SaaS (Software-as-a-Service)
  - Forge.mil
  - HBSS
- Enterprise Mall
  - Portal Services
  - Email
    - Active Directory / LDAP
    - Identity Lifecycle Manager (ILM)

DISA
A Combat Support Agency

RACE

- **Phase I IOC 15 Oct 08**
  - Basic Security – Zone B Enclave
  - Basic system admin for provisioning
  - Server Image
    - 1 CPU
    - 1 GB Memory
    - 50 GB Storage
    - O/S – STIG'd or UnSTIG'd
  - Windows or Linux
  - LAMP stack
  - Connectivity – NIPR
  - ATO/ATC Documentation
  - DECC Standards Documentation
  - Pilot - 480 servers/images or more
- **Phase II FY 09**
  - Higher Capacity Servers
  - Additional Optional Storage
  - Multi-tier/virtual network connectivity
  - Backup and COOP
  - Software
    - Application
    - Design Tools
    - Utilities
  - Services
    - Security
    - SA Support
    - T&D to Production transition support
  - Additional Zones/Enclaves
- **Expandable**
  - Add capacity to existing enclave
  - Create new enclaves for different security

RAPID ACCESS COMPUTING ENVIRONMENT

DISA
A Combat Support Agency

RACE Phase II Validation Zone

- The validation zone will be virtually separate from the T&D enclaves and management subnet
- A virtually separated firewall from the existing RACE enclave
- Separate VLANs within the transition zone to allow transition between
  - Zone B and zone A
  - Zone A to production
- A compliance checker within the zone to allow image validation prior to migration to the next zone

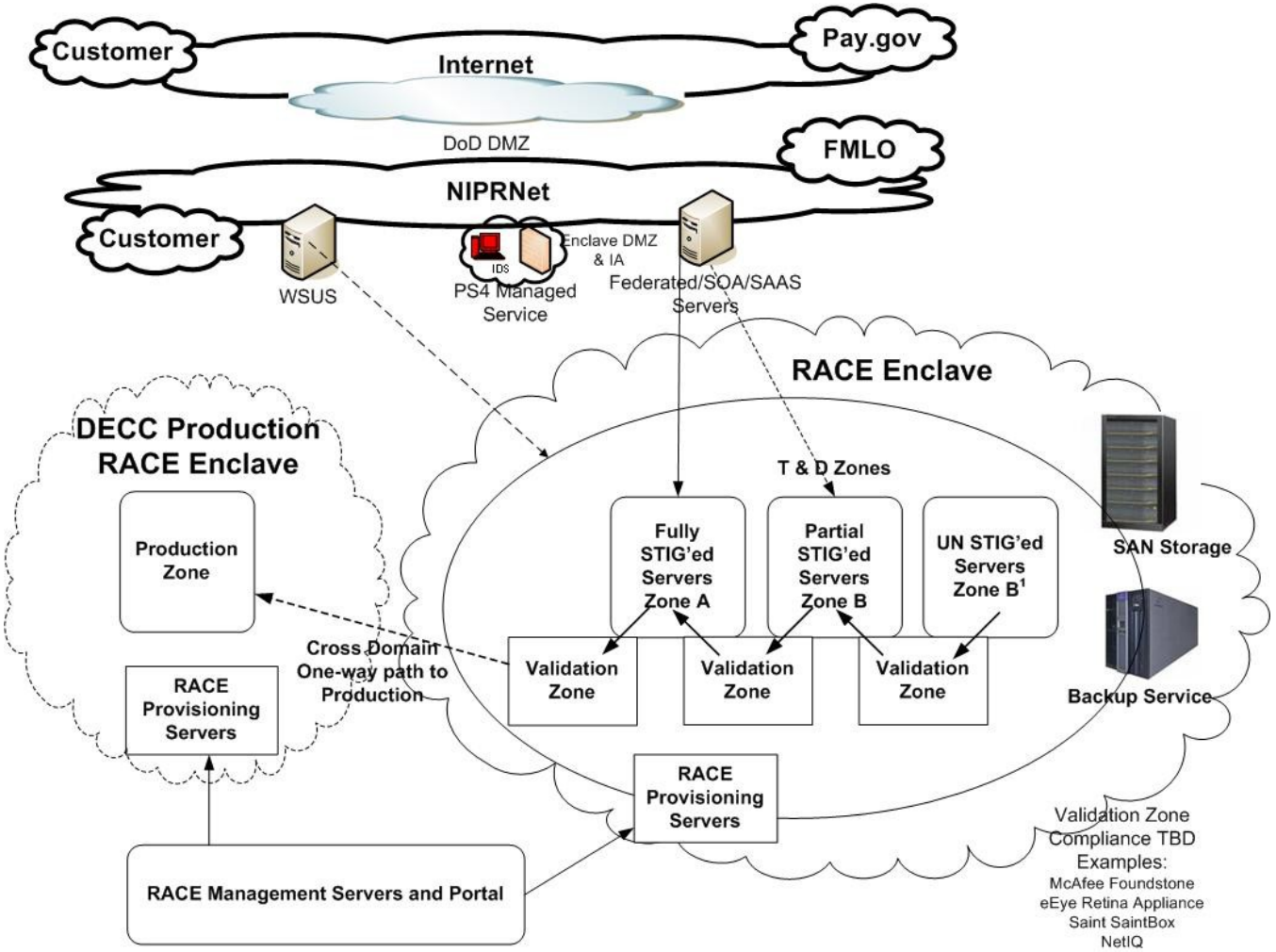
DISA
A Combat Support Agency

RACE Phase II Path to Production

- **Implement zones with varying connectivity**
  - **Zone B1 - UnSTIG, minimal connectivity per current RACE**
  - **Zone B - STIG, monitored external connections for testing – Federated servers**
  - **Zone A – Preproduction, fully STIG, in VMS process. Approved external connections, limited Web access for testing**
  - **Validation Zone – quarantine, CSD access only for image test and validation**

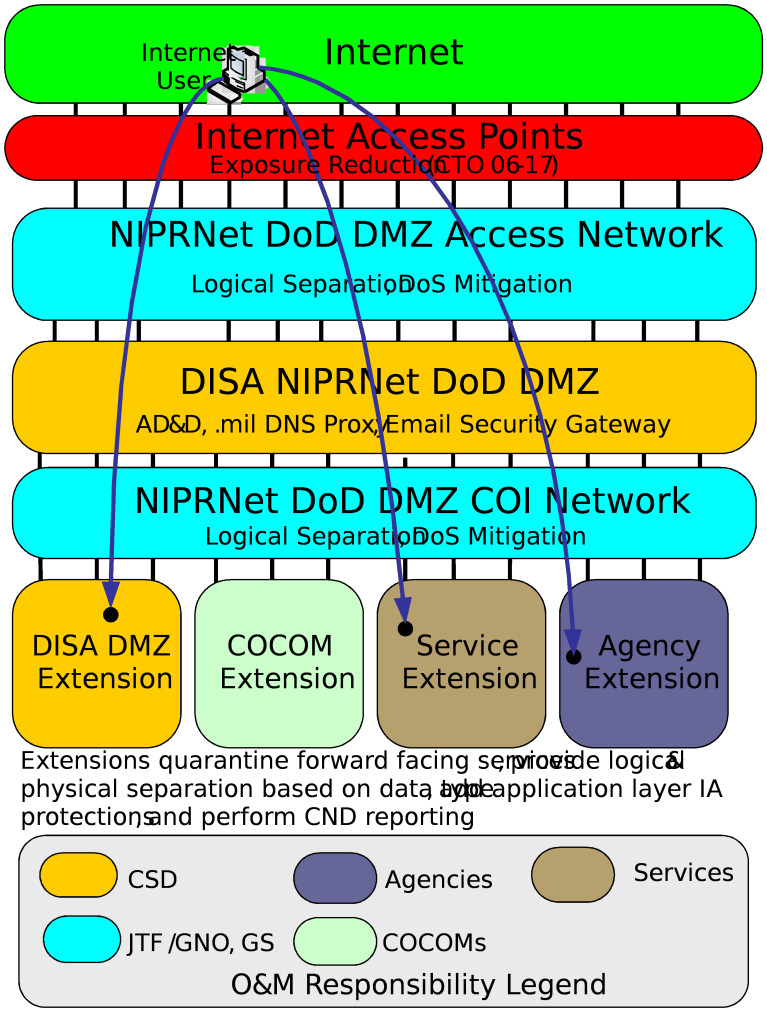
DISA
A Combat Support Agency

RACE Phase II Path to Production



NIPRNet DoD DMZ Target Architecture

A Combat Support Agency



- **NIPRNet DoD DMZ is comprised of the NIPRNet DoD DMZ front ends and NIPRNet DoD DMZ Extensions**
- **Applications can physically remain at the CC/S/A location, in a NIPRNet DoD DMZ Extension**
- **NIPRNet DoD DMZ access and COI networks logically connect the NIPRNet DoD DMZ components and stage the Internet facing applications at the Internet/NIPRNet boundary**
- **All inbound connections**

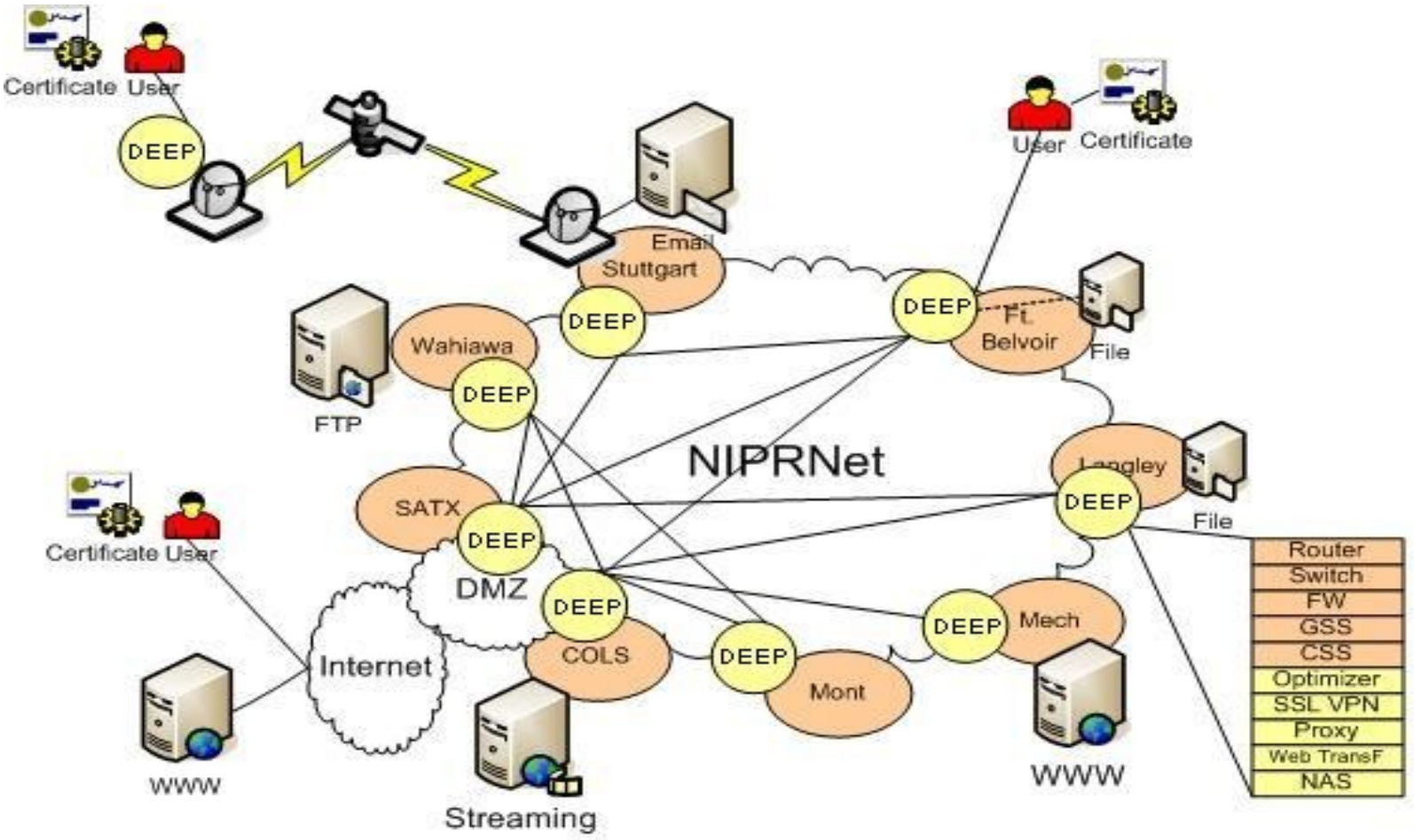
DISA
A Combat Support Agency

DISA Extended Edge Presence

- **Capabilities**
  - **Facilitates session services pushed further into the network beyond the DECC and DoD DMZ**
  - **Distributed DMZ like access to layer 4-6 services (Transport, Session, and Presentation)**
  - **Increased availability**
    - **Multiple geographically dispersed nodes to support the user base**
    - **DNS proximity used to determine the best available node**
  - **Provides agility and scalability**
    - **Type Accreditation**
  - **Increases management visibility to the Edge**
  - **Services**
    - **TCP optimization**
    - **Data proxy**
    - **On demand ad-hoc networks and network address storage (NAS)**
    - **Web services transformation**
    - **IPv6 conversion**

DISA Extended Edge Presence

A Combat Support Agency



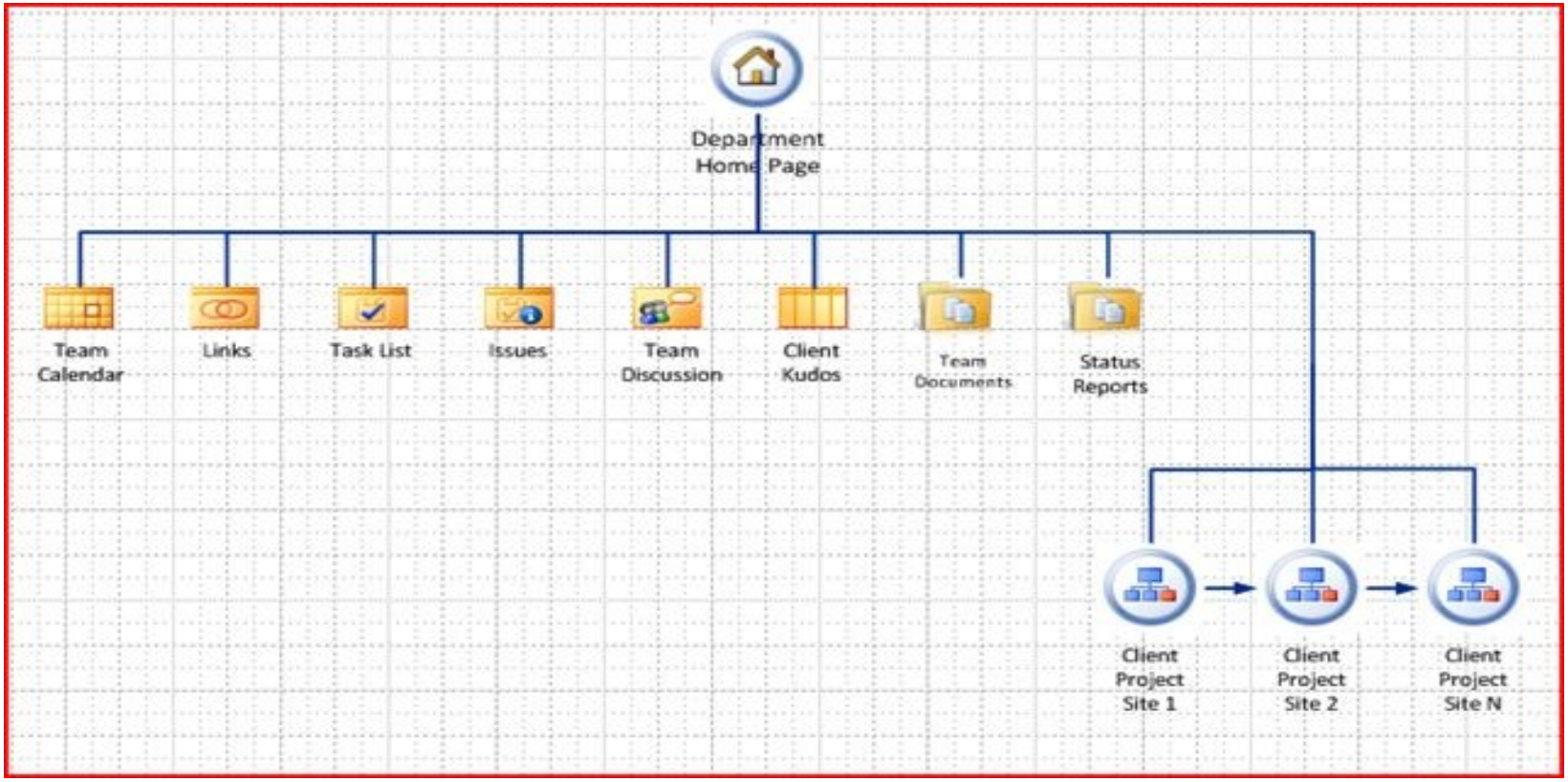
DISA
A Combat Support Agency

Portal Services

- **Capabilities**
  - **Provides all users with a single logical library**
  - **Cross Command collaboration**
  - **Single home page**
  - **Ownership and versioning is controlled through check-in and check-out process**
  - **Enterprise content repository**
  - **Document workflow**
  - **Communities of interest creation and replication**
    - **Application development platform**
    - **Calendar management**
    - **Task management**
    - **Records management**

DISA
A Combat Support Agency

Portal Services



Web Collaboration Store

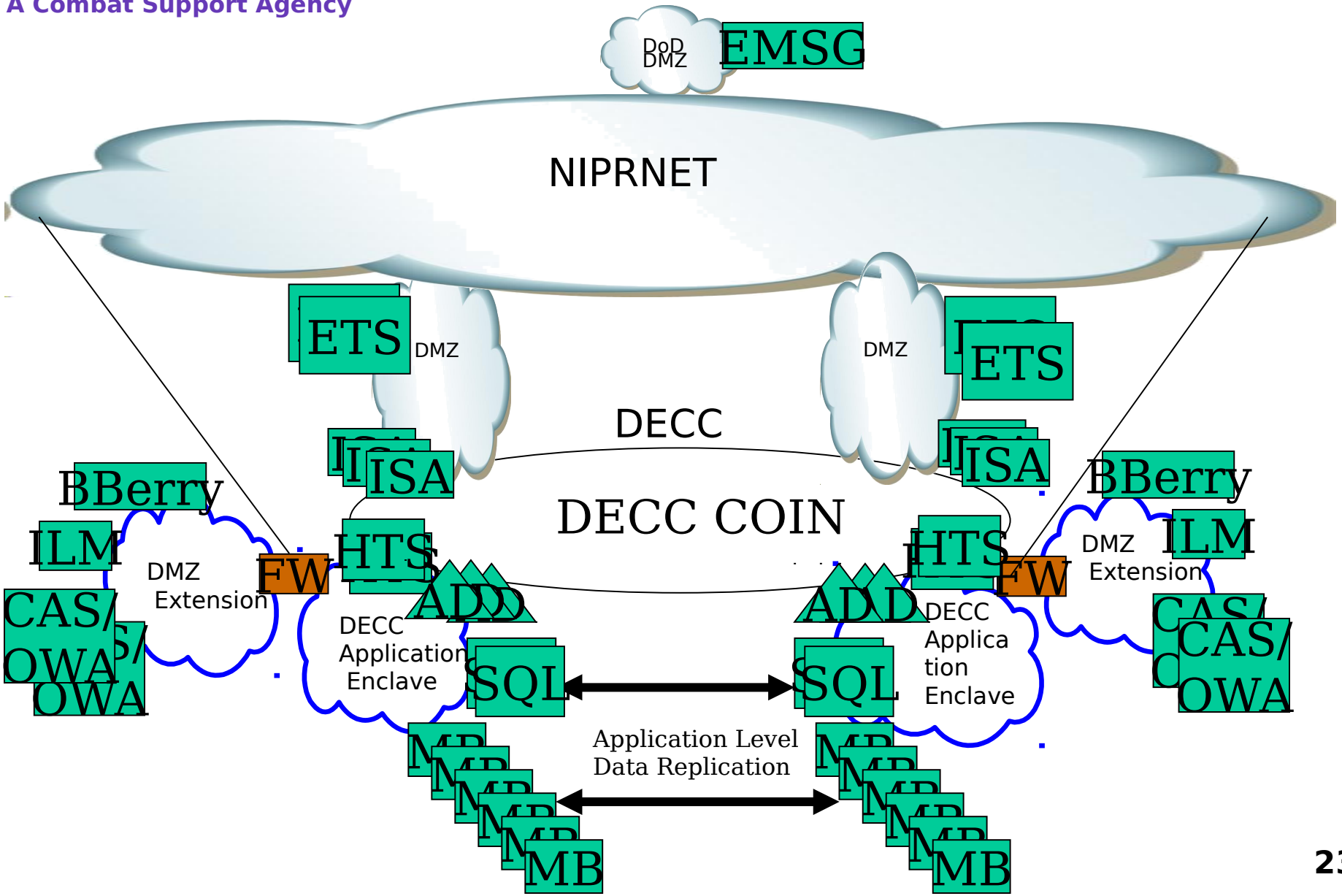
DISA
A Combat Support Agency

DoD Enterprise Email

- **Provide a robust, scalable and secure solution to the unclassified electronic messaging needs of the DoD Community**
- **Enhancing functionality, increasing availability and providing a highly functional business continuity solution**
- **Global email services will be provided for an expectation of 1,000,000 users**

DoD Enterprise Email

A Combat Support Agency



DEFENSE INFORMATION SYSTEMS AGENCY